ISSN Print: 2394-7500
ISSN Online: 2394-5869
Impact Factor: 5.2
IJAR 2017; 3(1): 669-672
www.allresearchjournal.com
Received: 17-11-2016
Accepted: 18-12-2016

Sakshi Aneja
KVA DAV College, Karnal, Haryana, India

Correspondence
Sakshi Aneja
KVA DAV College, Karnal, Haryana, India

Routing overview in MANETs

Sakshi Aneja

Abstract
MANET is a temporary wireless network composed of mobile nodes, in which there is no infrastructure. The mobile nodes can dynamically exchange data among themselves. Because of these characteristics, path connecting source nodes with destination may be very unstable and go down at any time, making communication over ad hoc networks difficult. Most of the routing protocols, despite of the belonging class (reactive, proactive, and hybrid), do not scale well when the number of nodes grows. Recently, some routing protocols have exploited the idea to decouple node identification from node's location (Dynamic Addressing) by resorting to Distributed Hash Table (DHT) services. This paper provides the overview of the DHT technique and provides a survey of the various DHT based routing protocols in MANETs.

Keywords: Manet, security, networking, protocols, reactive

Introduction
Stands for "Mobile Ad Hoc Network" A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission[7].

MANETs are decentralized mobile wireless networks comprised of computing devices that operate without any central administration or an access point. With the advance of technology and vast requirements of communication, research on wireless connectivity is focused on enabling mobile devices to connect with each other in absence of a central administration system. Due to the absence of fixed infrastructure, nodes setup routes among themselves autonomously. Nodes in a MANET move randomly and communicate directly with one another sharing the same media within their radio transmission range.

With the increase of portable devices as well as progress in wireless communication, ad hoc networking is gaining importance with the increasing number of widespread applications. Ad hoc networking can be applied anywhere where there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use. Ad hoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. MANETs can be exploited in a wide area of applications, from military, emergency rescue, law enforcement, commercial, to local and personal contexts.

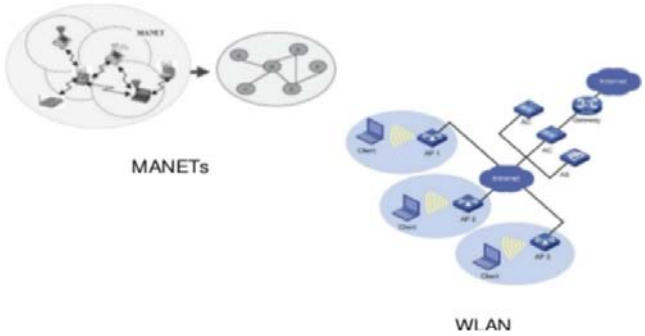

Fig 1: MANETs [1]

Due to the restricted transmission range of wireless network nodes, multiple hops are typically needed for a node to exchange information with any other node in the network. Thus routing protocols play significant role in ad hoc network communications. MANET is also called Mesh network. It is high adaptable and rapidly deployable network. [2]

Some MANETs are restricted to a local area of wireless devices (such as a group of laptop computers), while others may be connected to the Internet. For example, A VANET (Vehicular Ad Hoc Network), is a type of MANET that allows vehicles to communicate with roadside equipment. While the vehicles may not have a direct Internet connection, the wireless roadside equipment may be connected to the Internet, allowing data from the vehicles to be sent over the Internet. The vehicle data may be used to measure traffic conditions or keep track of trucking fleets. Because of the dynamic nature of MANETs, they are typically not very secure, so it is important to be cautious what data is sent over a MANET.

Routing Protocols in MANETs– MANET routing protocols could be broadly classified into three major categories: Proactive, hybrid and Reactive.

Proactive Routing Protocols (Table-driven): In Proactive routing protocols every node store information in the form of tables and when any type of change occur in network topology need to update these tables according to update. The node swaps topology information so they have route information any time when required. There is no route discovery delay associated with finding a new route. In proactive routing fixed cost generate, as normally greater than that of a reactive protocols. Proactive protocols use traditional distributed shortest-path protocols based on periodic updates. Proactive routing protocols are DSDV (destination sequenced demand vector), OLSR (optimized link state routing protocols) [S. A. Ade *et al*., 2010] [1].

Hybrid Routing Protocols: Hybrid routing protocols are combination of both reactive and proactive routing protocols. It was proposed to reduce the control overhead of proactive routing protocols and also decrease the latency caused by route discovery in reactive routing protocols. Hybrid routing protocols are ZRP (Zone routing protocol) and TORA (Temporarily Ordered Routing Algorithm). ZRP was planned to decrease the control overhead of proactive routing protocols and discovery in reactive routing protocols and also decrease the latency caused by route. It can be safely being assumed that most communication takes place between the node close to each other. ZRP provide framework to other protocols. The behaviour of ZRP is adaptive. ZRP based on the Zone, these are local neighbours each node within have many overlapping zones and each zone may have dissimilar size [Koushik Majumder *et al*., 2011] [14]

Reactive Routing Protocols: Reactive or on-demand routing protocols route is Discover when needed. Reactive protocols tend to decrease the control traffic messages overhead at the cost of increased latency to discover new routes. Source initiated route discovery in reactive routing protocols require less delay. In reactive protocols there is no need of distribution of information. It consumes bandwidth when transfer of data takes place from source to destination. Reactive Protocols are AODV (ad-hoc on demand distance vector), DSR (distance vector routing) and ABR (Associatively Based Routing) protocols.

Dynamic Addressing and DHT- Overview: Dynamic Addressing separates the routing address and the identity of a node. The routing address of a node is dynamic and changes with movement of the node to reflect the node's location in the network topology. The identifier is a globally unique number that stays the same during the lifetime of the node. Now the problem arises how to provide mapping between node identity and routing address. In fixed networks, location information can be easily embedded into the topological-dependent node address, which also uniquely identifies the node in the network. But in self-organizing networks, however, there is no permanent relationship between the location of the node and the node's identifier as a consequence of the spontaneity and adaptability of the network. So, this requires a dynamic association between identification and location of a node, and the specification of a mechanism to manage this association.

In response of needs, Distributed Hash Tables (DHTs) have been adopted as a scalable substrate to provide many functionalities including distribution of information, location service, and location-independent identity upon which a range of self-organizing systems have been built. The functionality of decoupling identification from location, and of providing a general mapping between them, has made the DHT as an interesting principle to be incorporated in network-level routing protocols. The key idea of DHT is to use a hash function to distribute Node's location information among rendezvous points throughout the network. This hash function is also used by a source to identify the point that stores a destination's location information.

DHT Based Routing Protocols In MANET- The following are the brief summaries of the protocols:

KDSR (Kademlia-based Dynamic Source Routing) is a DHT-based Dynamic Source Routing protocol for MANETs. Kademlia is seen as most widely deployed DHT-based protocol due to its simplicity and efficiency. KDSR combines Kademlia and DSR at the network layer to provide an indirect routing primitive for MANETs. KDSR assigns unique 160-bit node Ids to nodes. KDSR nodes store contact information about each other using the k-buckets. Each k-bucket includes k entries, which is kept sorted by time last read— least-recently read entry at the head, most-recently seen at the tail. Each entry in the k-buckets stores a vector of source routes to reach the designated NId. A KDSR entry is defined as a four-tuple:

Attribute	Description
NId	A unique hash identifier
IPAddr	The IP address of the node
SRoute	Multiple source routes to the node
Distance	The XOR distance to the node

In KDSR, a node always uses the newest among the shortest routes to send packets to the destination. KDSR not only uses explicit routes discovered through route discovery but also inherent route discovered through snooping and

overhearing to update the k-buckets. Kademlia uses a Least Recently Discovered (LRD) replacement algorithm to update the k-buckets. For routing in KDSR, a message key is first generated by hashing the destination IP address. The message key is used with XOR based routing algorithm for routing the message. Since both message keys and NIds are hashed from IP addresses, an exact match between a message key and the destination node's NId is expected. Each hop in KDSR route is a multi-hop source route. Each node in KDSR maintains a route cache constructed from the node's k-buckets. This allows the use of direct source routes to destinations, same as used in DSR. While routing if the route is available in the node's cache, it is used directly, otherwise X-OR based routing algorithm is used

MDART (Multipath Dynamic Address Routing)- MDART proactively discover all the available routes between a source and a destination. MDART assigns network addresses to all the nodes in the network based upon their position in the physical network topology. Network addresses are strings of bits, therefore we can represent address-space structure as a complete binary tree of l + 1 levels.

Complete binary tree is that tree in which every vertex has zero or two children and whose all leaves are at the identical level (Fig. 2- a). In the tree structure each leaf is associated with a network address. Every inner vertex of level k, that is a level-k sub tree, represents a set of network addresses sharing an address prefix of l – k bits.

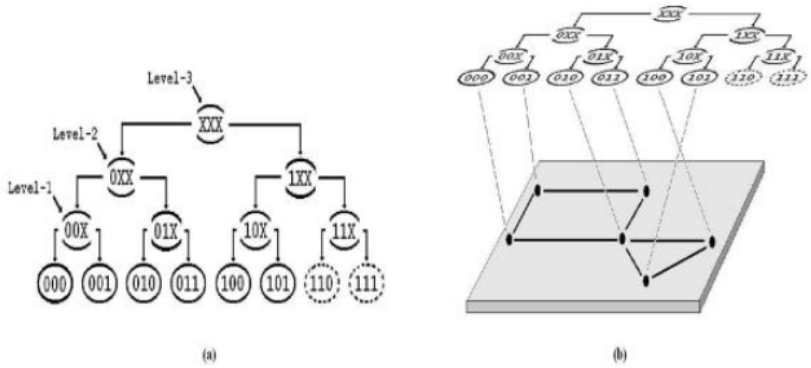

Fig 2: Relationship between Address space and Physical Topology [2]

For example, as we can see in Fig.2-a, the vertex having the label 01x is a subtree of level-1 and represents the leaves 010 and 011. We can define level-k sibling of a leaf as the level-k subtree sharing the same parent with the level-k subtree to which the leaf belongs. Thus, each address has onesiblings at all and each other address belonging to one and only one of these siblings. Referring to the earlier example, the address 000 has the vertex with the label 1xx as its level-2 sibling and the address100 belongs only to this sibling. In Fig. 2-b, the address space can be alternatively represented as an overlay network built upon the underlying physical network topology. Its tree-based structure offers manageable and simple procedures for address allocation, in this way it avoids to rely oninefficient mechanisms like flooding.

MDART provides each node with a routing table composed of l sections, one for each sibling, and the kthsection provides the path towards a node belonging to the level k sibling. Each section has five fields: the sibling to which the entry refers to, the next hop, the cost required to reach a node belonging to that siblingusing the next hop as or warder, the net_id used foraddress validation and the route log used by the loopavoidance mechanism.

DHT-OLSR (Distributed Hash Table-Optimized Link State Routing Protocol) [Ade, S.A & Tijare, P.A, 2010] [1] **-** is based on dynamic OLSR clustering enhanced with distributed hash tables routing based on MAD Pastry. The principle of this hybrid protocol is that each node runs OLSR locally within the cluster of nodes that are currently within a given number of hops. When a node wants to forward a packet headed for a destination that is not presently listed in the routing table maintained by OLSR, the node uses DHT-based unicast to immediately forward the packet to this remote destination. In other words we can say that the node do not buffer those packets. For this motive, each node running DHT-OLSR maintains a usual OLSR routing table, providing proficient and low delay routing. Whenever a node forwards a data packet, it first tries to search for the route in its OLSR routing table. If a legitimate route is found, the data packet is forwarded to the next hop on the path in the direction of the destination. In case no route could be found in the OLSR routing table, the node engages into the low maintenance overhead DHT routing scheme.

RRRP (Radio ring routing protocol)- is a DHT based routing protocol for mobile nodes in a MANET. RRRP works directly on top of the link layer using hexadecimal addresses. RRRP uses a DHT substrate for routing and therefore is an example of the structured overlay architecture. RRRP uses its DHT data structure for efficiently initializing the routing tables of the joining nodes to announce the entrance of new nodes. RRRP eliminates redundant breakdowns by a local repair method in which the nodes neighboring the link breakage work in the region of the problem without oncerning the end nodes. in addition, delete_keymessages make sure that routes are maintain edsymmetrically across two virtual neighbours.

Data replication is generally preserving data in case the node holding the data fails. If the node holding the data fails, the message will not be lost from the whole system. Routing recovery is a mechanism that handles node failures. In case of node failures, routing recovery algorithms repopulate the nodes' routing tables with live nodes. It removes stale routes and replaces them with updated routes. Static resilience in a DHT routing protocol occurs in the event of a node failure before the recovery algorithm takes

over. Static resilience is a good measure of time between a node failure and the start of the recovery algorithm. It also shows how well the protocol adjusts and works around a failure without the aid of any recovery mechanisms.

Conclusions and Future Work

The mobile ad hoc networks have been a subject of quite a number of investigations in recent years. Most of these investigations have been motivated by the need to design an efficient routing protocol for an ad hoc network. A good routing protocol needs to provide reliability and energy efficiency with low control overhead. In addition a good routing protocol also requires being scalable so that it should be able to operate efficiently as the network grows. To ensure scalability, many DHT based routing protocols have been proposed for MANET. This paper presented a survey of most recent DHT based routing protocols for MANETs.

We can conclude that M-DART is an efficient protocol. Its average energy consumption is lower. This protocol has the lowest delay due to its proactive nature. M-DART is scalable, as it supports large number of nodes. We have also found that when number of nodes grows, the performance of other multipath and unipath routing protocols while performance of M-DART is better in terms of Throughput, PDR, End to End Delay, Packet Loss and Hop Count.

Our future work will focus on the design of a DHT based routing protocol that will consider the advantages and weaknesses of the protocols mentioned in this paper. We will pay special attention to ease of routing, channel and energy efficiency.

References

1. Ade SA, Tijare PA. Performance Comparison of AODV, DSDV, OLSR and DSR International Journal of Information Technology and Knowledge Management. 2010.
2. Bouhorma, Mohammed, Bentaouit H, Boudhir A. Performance Comparison of Ad-hoc Routing Protocols AODV and DSR ‘, 2009 IEEE.
3. DHT based Routing Protocols for MANETs: A Survey[1Gurmukh Singh, Dr. Savita Gupta]
4. Zahn Schiller J. MAD Pastry. A DHT Substrate for Practicably Sized MANETs, in Proc. of ASWN, 2005.
5. Kush A, seema. New Scheme for Secured Routing in MANET” in International Journal of Computer Science, Engineering and Applications (IJCSEA). 2012, 2(4).
6. Kush A, Sima, Vishal. Securing Manet against Hacking, intlconf on applied and communication tech, Elsevier Publ, 2014, 121-126.
7. Sanjeev Prasad K, Karamjit Bhatia. RSAODV: A route Stability based Ad Hoc on Demand Distance Vector Routing Protocol for Mobile Ad hoc Network, International Journal of Wireless & Mobile Networks (IJWMN), 2014, 6(6).
8. Kush A, Sunil, Amandeep. Simulation Modeling of Reactive Protocols for Adhoc Wireless Network in the International Journal of Computer Science and Information Security (IJCSIS). 2010; 8(7):259-265. ISSN 1947-5500
9. Chatzigiannakis I, Nikoletseas SE, Spirakis PG. An efficient routing protocol for hierar-chical ad-hoc mobile networks, Proc. of the 15th International Parallel and Distributed Processing Symposium, 2001.
10. Frodigh M, Johansson P, Larsson P. Wireless ad hoc networking: the art of networking without a network Ericsson Review 2000; 4:248-263.
11. Yingyou W, Hong Z. KDSR: An Efficient DHT-based Routing Protocol for Mobile Ad Hoc Networks‖, Ninth International Conference on Hybrid Intelligent Systems, 2009, 245-249.
12. NZ Ali, Ahmad RB, Aljunid SA. A Survey on On-Demand Multipath Routing Protocol in MANETs”, International Conference on Electronic Design, 2008.
13. Kush A, Gupta P. Proposed Protocol for Secured Routing in Ad Hoc Networks Computer Science and Information Technology - Spring Conference, 2009. IACSITSC '09., IEEE Explore, DOI: 10.1109/IACSIT-SC. 2009; 28:76-81
14. Majumder, Koushik, Sudhabindu Ray, Subir Kumar Sarkar. Implementation and Performance Analysis of the Gateway Discovery Approaches in the Integrated MANET -Internet Scenario’, 2011 IEEE